العنوان:	الحماية الجنائية للتوقيع الإلكتروني في القانون الاتحادي رقم 2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات
المصدر:	مجلة الفكر الشرطي - مركز بحوث الشرطة - القيادة العامة لشرطة الشارقة - الإمارات
المؤلف الرئيسي:	محمد، خالد ممدوح إبراهيم
المجلد/العدد:	مج23, ع88
محكمة:	نعم
التاريخ الميلادي:	2014
الشهر:	يناير
الصفحات:	143 - 187
رقم MD:	606432
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الحماية الجنائية
رابط:	http://search.mandumah.com/Record/606432

الحماية الجنائية للتوقيع الإلكتروني

في القانون الاتحادي رقم 2 لسنه 2006م في شأن مكافحة جرائم تقنية المعلومات (المعدل بالقانون رقم 5 لسنه 2012) [1]

DOI:10.12816/0001936

الدكتور. خالد ممدوح إبراهيم محمد [2]

قاض بمحكمة الشارقة الاتحادية – الإمارات

مستخلص

أخذت العديد من الهيئات الدولية في الاعتبار المشكلات التي تواجه سلامة التوقيعات والمحررات الإلكترونية ، وقد بادر المجلس الاوروبى إلى وضع مشروع اتفاقية خاصة بجرائم الكمبيوتر، مع الأخذ في الاعتبار الطابع الدولي الذي يميز هذه النوعية من الجرائم . وبعد سنة ونصف تقريباً من المناقشات والتعديلات على هذا المشروع تم التوقيع على اتفاقية بودابست حيث قام المجلس الأوروبي بوضع اتفاقية بشأن الجرائم عبر الانترنت والمعروفة باسم اتفاقية بودابست 2001 ، حيث تعنى الاتفاقية بضرورة أن يقر كل طرف الإجراءات التشريعية وغيرها التي تبدو لازمة ، وفقاً لقانونه الداخلي ، لتحديد الفعل الذي ينتج عنه عمداً وبدون وجه حق جريمة إتلاف أو مسح أو تدمير أو تعديل أو إلغاء لبيانات معلوماتية . ومن جهة أخرى ، أخذ قانون العقوبات الفرنسي بعين الاعتبار لنوعين من الجرائم الماسة بسلامة المحرر الإلكتروني، وذلك من خلال مسايرة التوصيف التقليدي "للتزوير" للوسط الإلكتروني ، ومنع أعمال الغش في شأن البيانات. وفي ذات الاتجاه ، أفرد قانون التوقيع الإلكتروني المصري تجريماً للمساس بالتوقيع الإلكتروني . ومن أشهر صور الاعتداء على التوقيع الإلكتروني إتلاف التوقيع الإلكتروني ، والتزوير أو التقليد ، والدخول غير المشروع علي أنظمة معلوماتية أو قواعد بيانات خاصة بالتوقيع الإلكتروني. وقد بادر المجلس الاوروبى إلى وضع مشروع اتفاقية خاصة بجرائم الكمبيوتر، مع الأخذ في الاعتبار الطابع الدولي الذي يميز هذه النوعية من الجرائم ، وبعد سنة ونصف تقريباً من المناقشات والتعديلات على هذا المشروع تم التوقيع على اتفاقية بودابست بتاريخ 23 نوفمبر 2001 بشأن الإجرام المعلوماتي ، وذلك إيماناً من الدول الأعضاء في المجلس الاوروبى والدول الأخرى الموقعة على هذه الاتفاقية بضرورة مواجهة هذا النمط الجديد من الأجرام .

مفردات البحث:

الحماية الجنائية — التوقيع الإلكتروني — الجرائم المعلوماتية — إتلاف التوقيع الإلكتروني — تزوير التوقيع الإلكتروني — الدخول غير المصرح على قاعدة بيانات التوقيع الإلكتروني.

1- ورد هذا البحث للدورية في ديسمبر 2011م وقيد تحت رقم 2011/2 وأحيل للتحكيم في فبراير 2012م وأجيز للنشر في يناير 2013م.

2- حصل الدكتور خالد ممدوح على درجة الدكتوراه في القانون من جامعة إسكندرية بمصر كما حصل على شهادة من وزارة التجارة الأمريكية في معاملات التجارة الإلكترونية وشهادة في حقوق الملكية الفكرية من برنامج تنمية القانون التجاري بأمريكا وحصل على شهادة من دولة سنغافورة في إدارة نظم التقاضي الإلكتروني وإجراءات المحاكم وهو محاضر ومحكم وله العديد من الأبحاث والدراسات في مجال الجرائم الإلكترونية.

Legal Protection of E. Signature as per Federal Law No 2 of 2006 concerning IT Crimes Combat, amended by Law No 5 of 2012 [1]

DOI:10.12816/0001936

Dr. Khalid Mamdooh Ibrahim Mohammed [2]
A judge at Sharjah Federal Court – UAE

Abstract:

Problems facing security of E signatures have been considered by international authorities; Council of Europe has blazed a trail by setting a draft convention on cybercrimes, taking into consideration the global nature of such crimes. Budapest 2001 Convention on Cybercrimes was signed after one year of discussions and amendments of the previous draft convention. Budapest Convention stipulated that each party should acknowledge required legislative procedures as per its bi laws to determine acts resulting in intentional damage, deleting, destroying or cancellation of data. On the other hand, French Penal Code has taken into account two kinds of crimes concerning security of electronically executed agreements by adopting the traditional description of (forgery) and preventing data- related fraud. Egyptian Electronic Signature Law has criminalized tampering with E signature, and the most common forms of electronic signature abuse are damage, forgery and imitation as well as the unauthorized access to information systems or data bases belonging to the E. Signature.

Keywords:
Criminal Protection – E- Signature – Information – Related Crimes – Damage of E- Signature – Forgery of E- Signature – Unauthorized Access to Data Bases of the E. Signature.

1-**Manuscript:** was submitted in December 2011 under No 2/2011, refereed in February 2012 and approved for publication in January 2013.

2-**Biography:** Dr. Khalid Mamdooh attained his PhD in Law from Alexandria University and a certificate from USA Department of Commerce in Electronic Trade Transactions, and another in Intellectual Property Rights from USA Commercial Law Development Program. He also got a certificate in Electronic Prosecution System and Court Procedures from Singapore. He is a lecturer and arbitrator who published a host of researches and studies in the arena of cybercrimes.

مقدمة :

لاشك أن تحقيق الحماية الجنائية للتوقيع الإلكتروني من المخاطر التي تتهدده يؤدى إلى تحقيق الاستقرار والأمان القانوني للمعاملات الإلكترونية ، ويرجع ذلك إلى أن كفالة الحماية القانونية الكاملة للتوقيع الإلكتروني هو أمر من شأنه أن يكفل للأفراد الطمأنينة واستقرار المعاملات ، ويؤدى إلى أن يصير هذا التوقيع دليلاً في الإثبات أمام المحاكم يقف على قدم المساواة مع التوقيع التقليدي.

ونظراً لانتشار الجرائم المعلوماتية Cyber Crime ، أخذت العديد من الهيئات الدولية في الاعتبار المشكلات التي تواجه سلامة التوقيعات والمحررات الإلكترونية ، فمثلاً قام المجلس الأوروبي Conseil de l'Europe بوضع اتفاقية بشأن الجرائم عبر الإنترنت Cybercriminalité [1] والمعروفة باسم اتفاقية بودابست 2001 ، حيث تعني المادة الرابعة من هذه الاتفاقية في فقرتها الأولى بضرورة أن يقر كل طرف الإجراءات التشريعية وغيرها التي تبدو لازمة ، وفقاً لقانونه الداخلي ، لتحديد الفعل الذي ينتج عنه عمداً وبدون وجه حق جريمة إتلاف أو مسح أو تدمير أو تعديل أو إلغاء لبيانات معلوماتية.

ومن جهة أخرى ، أخذ قانون العقوبات الفرنسي بعين الاعتبار لنوعين من الجرائم الماسة بسلامة المحرر الإلكتروني ، وذلك من خلال مسايرة التوصيف التقليدي "للتزوير" للوسط الإلكتروني ، ومنع أعمال الغش في شأن البيانات. وفي ذات الاتجاه ، أفرد قانون التوقيع الإلكتروني المصري تجريماً للمساس بالتوقيع الإلكتروني.

ومن أشهر صور الاعتداء على التوقيع الإلكتروني إتلاف التوقيع الإلكتروني ، والتزوير أو التقليد ، والدخول غير المشروع على أنظمة معلوماتية أو قواعد بيانات خاصة بالتوقيع الإلكتروني ، ونتناولها على نحو ما يلي.

1- La Convention sur la cybercriminalité, un outil de coopération internationale unique, 2001, disponible sur le site de conseil de l'Europe suivent: http://www.coe.int/NewsSearch/Default.asp?p=nwz&id=802&lmLangue=1

المبحث الأول
جريمة إتلاف التوقيع الإلكتروني

حرص **المشرع الإماراتي** على تجريم إتلاف التوقيع الإلكتروني بصورة مباشرة **في القانون الاتحادي رقم 2 لسنه 2006 في شأن مكافحة جرائم تقنية المعلومات** [1] ، ونعرض في هذا المجال إلي مفهوم وأركان جريمة الإتلاف التقليدية ثم نعرض بعد ذلك إلى مفهوم وأركان جريمة الإتلاف المعلوماتي للتوقيع الالكتروني.

أولاً - مفهوم وأركان جريمة الإتلاف التقليدية:

الإتلاف بصفة عامة هو تخريب الشيء محل الجريمة وذلك بإتلافه أو التقليل من قيمته وذلك بجعله غير صالح للاستعمال أو تعطيله [2]. وعرف بعض الفقه الإتلاف بأنه " التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له [3]. والركن المادي لجريمة الإتلاف يتكون من فعل مادي وهو الإتلاف ومحل الجريمة هو المال الثابت أو المنقول وأن يكون هذا المال مملوكاً للغير وسنتناول هذا الركن بشيء من التفصيل ، ومن ثم نتناول القصد الجنائي الواجب توافره لقيام جريمة الإتلاف. وقد ذكر المشرع عدة صور للفعل الذي يقوم به الركن المادي لجريمة الإتلاف وهذه الصور هي هدم المال – إتلاف المال – جعل المال غير صالح للاستعمال – وتعطيل المال بأية طريقة. وهذه الصور تكاد تكون مرتبطة مع بعضها البعض فقد يقع الإتلاف على جزء من المال وتقوم الجريمة بشرط أن يكون من شأن هذا الإتلاف جعل المال غير صالح للاستعمال أو تعطيله.

ثانياً - أركان جريمة إتلاف التوقيع الإلكتروني:

نصت المادة الثانية من **القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات** على تجريم **كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام**

1- عدلت بعض نصوص هذا القانون بموجب القانون الاتحادي رقم 5 لسنة 2012 الصادر بتاريخ 2012/8/13 والمنشور بالجريدة الرسمية في العدد 540 ملحق في 2012/8/26 ص19.

2- د. نجيب حسني ، قانون العقوبات ، دار النهضة العربية ، 1987 ، ص107.

3- د. جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية ، 2002 ، ص127.

معلوماتي..... يعاقب بالحبس فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس.... ". أي أن المشرع الإماراتي قد عاقب على هذه الأفعال بوصف الجنحة.

وقد شدد **المشرع الإماراتي** من هذه العقوبة حالة كون من ارتكب هذه الجريمة موظفاً مسؤولاً مما يعمل في إحدى جهات تشغيل التوقيع الالكتروني ، حيث جاء نص المادة (3) **من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** على أن "**كل من ارتكب أيا من هذه الجرائم المنصوص عليها في البند (2) من المادة (2) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين**".

ولم تكــن المادة السابقة هي المادة الوحيدة التي تناولت **جريمة إتلاف التوقيع الإلكتروني**، حيث جاء نص المادة **(6) من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** على أن كل من ادخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف **أو إتلاف** أو تعديل **البرامج أو البيانات أو المعلومات فيها** يعاقب بالسجن المؤقت وبالغرامة.....". ويلاحظ أن **المشرع الإماراتي** قد اعتبر – وبطريق غير مباشر – أن الدخول على شبكة الإنترنت بواسطة برامج خاصة أو فيروسات بطرق تؤدي إلي إتلاف البرامج بصفة عامة – ومنها برامج تشغيل التوقيع الالكتروني – جريمة يعاقب عليها بعقوبة

وسوف نتناول الإشارة أولاً إلى الركن المادي لجريمة إتلاف المعلومات ثــم نتعــرف على الركن المعنوي وذلك من خلال النصوص المختلفة التي جرمتهما.

(أ) الركن المادي لجريمة إتلاف التوقيع الإلكتروني:

قد يتخذ الركن المادي لجريمة إتلاف معلومات التوقيع الإلكتروني إما صورة إجــراء تعديلات غير مشروعة لها Modification ، أو تــدميرها Destruction ، أو الإدخــال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية Introduction.

1- التعديل غير المشروع لمعلومات التوقيع الإلكتروني:

يشكل التعديل غير المشروع للمعلومات المبرمجة آلياً واحداً من أكثر صور إتلاف المعلومات شيوعاً ، ويمكن تعريفه بأنه كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الكمبيوتر. وقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلقة بجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات والبرامج وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من برامج الكمبيوتر ونظامه.

2- تدمير المعلومات المدرجة بالتوقيع الإلكتروني:

يعد تدمير المعلومات صورة من صور الإتلاف ، وإن كان أبعد أثراً من مجرد إجراء بعض التعديلات للمعلومات ، وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات ، ولقد ميزت التوصية الصادرة عن المجلس الأوروبي بين شكلين من أشكال التدمير الذي يلحق بالمعلومات ، الأول يتعلق بمحو المعلومات تماماً ، والثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تماماً. ويذهب البعض إلى أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تدميراً لها ، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو المعلومات التي يحتوي عليها من ذاكرة الكمبيوتر ، وإنما يؤدي فقط إلى تعديل في قائمة الملفات وهو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو أن يكون تعديلاً وليس تدميراً [1].

3- الإدخال غير المشروع لمعلومات التوقيع الإلكتروني:

إذا كان تعديل المعلومات ومحوها وإخفاؤها قد يشكل إتلافاً لها فهل يمكن أن يترتب علي إدخال المعلومات والبرامج إتلاف لأي من المكونات المنطقية للحاسب الآلي ؟ الواقع أن الإدخال غير المشروع للمعلومات أو البرامج قد يترتب عليه فضلاً عن التعديل الذي

1-Vergutch Pascal , Op. cit., p 222.

يطرأ على ذاكرة الحاسب الآلي تعديلاً للمعلومات ذاتها أو تدميراً لها كما في حالة إدخال برامج خبيثة إلى نظام الكمبيوتر.

(ب) الركن المعنوي في جريمة إتلاف التوقيع الإلكتروني:

يشترط لقيام هذه الجريمة توافر القصد العام فيكفي هذا القصد لثبوت علم الجاني بأن التوقيع الالكتروني التي يعتدي عليه بالإتلاف هي ملك الغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطلاً أو يجعله غير صالح للاستعمال أو ينقص قيمته ، ويجب أيضاً أن **تتجه إرادة الجاني** إلى إحداث الإتلاف أو التخريب أو التعطيل وينتج عن فعله تحقق الضرر المترتب على جريمته مع علمه أن فعله غير شرعي [1].

ويجب أيضاً اتجاه الإرادة نحو القيام بالفعل الذي يؤدي إلى الإتلاف ، فالمادة 2/423 ، 3 (عقوبات فرنسي) تتطلب القصد الجنائي لأن الجريمة عمدية ففي الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بالاعتداء على المعلومات الموجودة داخل الجهاز تتجه إرادة الجاني إلى إتلاف المال وذلك بالقيام بوضع برنامج من شأنه أن يغير المعلومات أو يقوم بمحو البيانات فمن يعمل هذا العمل الإجرامي فهو على درجة عالية من الناحية التقنية في مجال المعلوماتية [2].

ثالثاً - وسائل إتلاف المعلومات المبرمجة بالتوقيع الإلكتروني:

تتعدد وسائل إتلاف المعلومات أو برامج أنظمة المعالجة الآلية للمعلومات ، ولعل أهم هذه الوسائل وأكثرها ضرراً هو استخدام الفيروسات ولذا سوف نتناوله استقلالاً ، ثم نبين باقي الوسائل التي قد تستخدم لإتلاف المعلومات.

1- د. عبد المهيمن بكر ، جرائم الكمبيوتر ، دار القانون ، 2009 ، ص182.

2- د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، 2009 ، 432 وما بعدها.

1- الإتلاف بواسطة استخدام البرامج الخبيثة (الفيروسات) :

الفيروسات هي برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة للاتصالات بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم وهو يسمى عادة باسم أول مكان اكتشف فيه. والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها ، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها وعلى الرغم من تدميرها للبرامج والمعلومات ، إلا أنها لا تسبب عادة تدميراً لأي من المكونات المادية للنظام. وتستخدم كلمة الفيروس في مجال المعلوماتية بشكل عام للدلالة على كل البرامج الخبيثة التي تسبب إتلافاً لأنظمة المعالجة الآلية للمعلومات إلا أن الفيروس Virus في حقيقة الأمر هو أحد أنواع هذه البرامج والتي تشمل إلى جانبه البكتريا Bacterium الديدان Worms حصان طروادة Trojan Horses والقنابل المنطقية Logic Bombs ، وتتسبب هذه البرامج جميعاً في إتلاف المكونات المنطقية للكمبيوتر وتستمد التفرقة بين هذه البرامج أساسها من أسلوب كل منهم في أداء مهمته فالفيروس هو برنامج قادر على التكاثر وإرسال النسخ الجديدة إلى أنظمة أخرى بحيث يصبح معرفة مصدره أمراً بالغ الصعوبة [1].

والفيروسات التي تصيب جهاز الكمبيوتر متعددة ويمكن تقسيمها إلى حيث تكوينها وأهدافها إلى ما يلي: [2]

أ- **فيروس عام الانتشار:** وهو يصيب أي برنامج أو ملف داخل الكمبيوتر.

ب- **فيروس محدود الانتشار:** وهو يصيب نوعاً معيناً من النظم ويتميز عن سابقة بالبطء في الانتشار وصعوبة اكتشافه.

1- Davies David , Computer Virus-The Major Computer Abuse Threat of 1988 ?, C.L.S.R. , 1988-89, p.2, Fish Nigri Deborah , Op. Cit., p. 190.

2- د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994 ، ص191.

ج- **فيروس عام الهدف** : يمتاز بسهولة إعداده واتساع مدى تدميره والغالبية العظمى من الفيروسات تندرج تحته.

د- **فيروس محدد الهدف** : وهذا النوع من الفيروسات يقوم بتغيير الهدف من عمل البرنامج دون أن يعطله.

2- الإتلاف الطبيعي للتوقيع الإلكتروني: [1]

فضلاً عن استخدام البرامج الخبيثة كوسيلة لإتلاف المكونات المنطقية للحاسبات الآلية توجد وسائل أخرى يتم الاستعانة بها من أجل إحداث هذا التلف ، ونذكر منها على سبيل المثال محو البيانات عن طريق تعريض الأسطوانات أو الأقراص الممغنطة المسجلة عليها لقوى مغناطيسية أو قطع التيار أثناء معالجة البيانات أو وضع شريحة أو دائرة مطبوعة في غير مكانها الصحيح.

كذلك قد يحدث تحريف طبيعي ناشئ عن ضعف الدعامة أو المادة المثبت عليها المحرر أو التوقيع ، أو حدوث خلل فى الأنظمة المعلوماتية أثناء إرسال المحرر ترتب عليه إتلافه أو تدميره ، فقد يحدث في الواقع العملي أن تفسد سلامة المحرر نتيجة حدوث أي ضرر بدعامته الإلكترونية ، والذي قد ينشأ على سبيل المثال عن سوء اختيار دعامة جيدة للحفظ توفر استدامة للمعلومات المدونة عليها ، كما قد يتلف المحرر أثناء تبادله بين الأطراف عبر الشبكة من جراء الصيانة السيئة للخطوط أو الأجهزة الطرفية للنظام المعلوماتى. يضاف إلى ذلك ، أن الأنواع المختلفة للدعامات الإلكترونية المستخدمة فى حفظ المحرر الإلكتروني لها مدة صلاحية محددة [2] ، ومن ثَمَّ فإن نقل المعلومات على دعامة جديدة للحفظ في وقت مناسب ، يعتبر ضرورياً في هذا الصدد ، وإلا من المحتمل أن يُصبح مضمون المحرر موضوعاً لتحريف بالغ.

1- د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، 442 وما بعدها.

2- Voir : Isabelle DE LAMBERTERIE, Preuve, conservation et archivage, in Une société sans papier ? Nouvelles technologies de l'information et droit de la preuve, La Documentation Française, Paris, 1990, p. 238.

3- الإتلاف الناتج عن الخطأ البشري:

يشكل الخطأ البشري أحد صور إتلاف التوقيع الإلكتروني ، لارتباطه بعملية إدخال البيان أو المعلومة فى وسيلة الاتصال ، فهذه تعتمد العملية في الغالب على الإدخال اليدوي. كما قد يرجع الخطأ إلى الاستخدام السيئ – من قبل القائمين على النظام – لبرامج الحاسوب أو الأجهزة المعدة لنقل المعلومات التي تربط بين أنظمة معلوماتية متعددة ، كما يمكن تصور الغلط أيضاً في مرحلة إرسال المحرر الإلكتروني أو في مرحلة حفظه. ويبدو في هذا الصدد ، أهمية إبداء النصح للمستخدمين باللجوء إلى أحد مقدمي خدمات التصديق الإلكتروني الذي يوفر لهم ضمانات عديدة في شأن موثوقية المحرر الالكتروني والتوقيع الالكتروني [1].

رابعاً - موقف بعض التشريعات الأجنبية من جريمة إتلاف معلومات التوقيع الإلكتروني:

بشكل عام يمكن أن نلاحظ أن التشريعات المختلفة قد ميزت بين إتلاف المعلومات والبرامج من ناحية وإعاقة أنظمة الحاسبات الآلية من ناحية أخرى. فبينما اتجهت بعض الدول كفرنسا ولوكسمبورغ وألمانيا والبرتغال وهولندا وإيطاليا واليابان إلى تجريم كل من السلوكيين بنصوص منفصلة ، اتجهت دول أخرى إلى تعديل النصوص التقليدية الخاصة بجريمة الإتلاف وإدراج السلوكين معاً في هذه النصوص كأستراليا وكندا وتركيا ، واكتفت دول أخرى كفنلندا والمملكة المتحدة والنمسا والسويد وهولندا وإسبانيا وسويسرا بتجريم الإتلاف الواقع على المعلومات والبرامج وتباينت فيما بينها من حيث مدى قابلية نصوصها للتطبيق في حالة إعاقة نظام الحاسب الآلي ، ونعرض إلي بعض هذه التشريعات.

1- الولايات المتحدة الأمريكية :

لم يحتو التشريع الفيدرالي في الولايات المتحدة الأمريكية قبل عام 1986 على تجريم لإتلاف المعلومات والبرامج ، وإنما اقتصر التجريم على إعاقة أنظمة الحاسبات الآلية ، فقد

1- Voir:S. CAÏDI, La preuve et la conservation de l’écrit dans la société de l’information, op. cit., p. 55.

جرمت الفقرة الثالثة من المادة 1030 (أ) من القانون الفيدرالي لجرائم الحاسبات الآلية الصادر عام 1984 إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية وفي عام 1986.

ونتيجة لكثير من الانتقادات التي وجهت إلى القانون الصادر عام 1984 تم تعديله وأصبحت الفقرة الثالثة من المادة 1030 (أ) تتناول فقط الدخول غير المصرح إلى حاسب آلي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال ، وأضيفت فقرة خامسة إلى المادة 1030 (أ) تتناول جريمة الإتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها كمبيوتر تابع لحكومة الولايات المتحدة وإداراتها أو كمبيوتر غير تابع للحكومة ، إلا أنه يتم استخدامه من قبلها أو لصالحها أو إعاقة هذا الكمبيوتر عن أداء المهام المختلفة التي تباشرها الحكومة بواسطته.

وقد أضيفت الفقرة السابقة لحماية المعلومات وأنظمة الحاسبات الآلية من أعمال الإتلاف التي ترتكب بواسطة أشخاص غير مصرح لهم بالدخول إلى النظام Outsiders وذلك في حالتين : الأولى أن يترتب على أعمال الإتلاف خسارة مادية تقدر بألف دولار أو أكثر خلال مدة عام واحد ، والثانية أن تتعلق أعمال الإتلاف بمعلومات طبية دون اعتبار للخسائر المادية الناجمة عن ذلك [1].

2- فرنسا:

تناولت المادتان 462 – 3 و 462 – 4 من القانون رقم 19 لعام 1988 الخاص بجرائم المعلوماتية – اللتان حلت محلهما المادتان 323–2 و 323–3 من قانون العقوبات الفرنسي الجديد – إعاقة أنظمة الحاسبات الآلية والإتلاف الواقع على المعلومات باعتبارهما جريمتين مستقلتين فقد تناولت المادة 462–3 جريمة إعاقة أنظمة الحاسبات الآلية عن أداء وظيفتها حيث نصت على أنه : (يعاقب بالحبس مدة تتراوح بين ثلاثة شهور وثلاث سنوات

1- Griffith Dodd S. The Computer Fraud and Abuse Act of 1986 : A Measured Response to a Growing Problem, V.L.Rev. 43, p. 453.

وبغرامة تتراوح بين 10.000 و 100.000 فرانك كل من قام عمداً وبدون مراعاة لحقوق الغير بإعاقة أو إفساد نظام للمعالجة الآلية للمعلومات).

فبموجب هذه المادة يتم تجريم كافة الأفعال التي من شأنها أن تؤدي إلى الحيلولة دون أن يعمل نظام المعالجة الآلية للمعلومات على الوجه المحدد له ، ومن ثم لا يقتصر التجريم على الأفعال التي تؤدي إلى إتلاف النظام أو إفساده بل يشمل أيضاً الأفعال التي تؤدي إلى الحيلولة دون الوصول إلى النظام أما المادة 462-4 فقد تناولت إتلاف المعلومات حيث نصت على أنه: (يعاقب بالحبس مدة تتراوح بين ثلاثة شهور وثلاث سنوات وبغرامة تتراوح بين 2000 و 500.000 فرانك أو بإحدى هاتين العقوبتين كل من أدخل عمداً إلى نظام المعالجة الآلية للمعلومات بطريق مباشر أو غير مباشر وبدون مراعاة لحقوق الغير بيانات أو محا أو عدل في البيانات التي يحويها أو في طريق معالجتها أو نقلها).

ويلاحظ أن المشرع الفرنسي لم يضع شروطاً تتعلق بطبيعة المعلومات محل الإتلاف [1] ، بل ترك النص عاماً ليتسع لكافة أنواع المعلومات ، كما أن طرق إتلاف المعلومات الواردة به تتسع لتشمل كافة أشكال الاعتداء على المعلومات بما في ذلك استخدام البرامج الخبيثة أياً ما كانت وسيلة إدخالها إلى نظام الحاسب الآلي [2].

3- المملكة المتحدة:

ظهرت الحاجة في المملكة المتحدة إلى نصوص خاصة بإتلاف المعلوماتي بعد قضية Cox v. Riley ، وما أثارته من شك حول مدى صلاحية الاتجاه الذي اتخذته المحكمة للتطبيق في حالة إتلاف المكونات المنطقية للكمبيوتر.

1- Bibent Michel , Le Droit du Traitement de l’Information, 2000, p. 121.

2-Chamoux Francoise, la loi sur la Fraude Informatique De Nouvelles Incriminations, Jcp,1988 , I, Doctrine 3321, No 9 ; Linant de bellefonds xavier & Hollande Alain Pratique du Droit de l’informatique, 1998, p. 238.

وقد أسفر هذا الوضع عن تبني المادة الثالثة من قانون إساءة استخدام الحاسبات الآلية لعام 1990 ، والتي تنص فقرتها الأولى على أنه يعد مرتكباً لجريمة الإتلاف المعلوماتي "كل من يقوم بعمل من شأنه إحداث تغييرات غير مصرح بها في محتوى أي حاسب آلي متى توافر لديه العلم والإرادة وقت قيامه بهذا الفعل". وبالنظر إلى هذه المادة يتبين لنا أنها تتطلب أن تكون الأفعال التي يقوم بها الفاعل غير المصرح بها ، بمعنى أن الفاعل غير مصرح له بإحداث أي تغيير يتعلق بالمعلومات ، فالعبرة هنا لمشروعية السلوك أن يكون التصريح منصباً على تغيير المعلومات وليس مجرد التصريح بالدخول إلى المعلومات ، والقول بعكس ذلك يؤدي إلى أن الموظف المصرح له بالدخول إلى نظام الكمبيوتر الخاص برئيسه دون أن يتعدى ذلك أن تغيير المعلومات التي يحتوي عليها النظام يستطيع تغيير هذه المعلومات وإتلافها دون أن تنطبق بشأنه المادة سالفة الذكر.

4- سلطنة عمان:

نص القانون العماني للمعاملات الإلكترونية رقم 69 لسنة 2008 في المادة (3/52)" مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر يعاقب بالسجن لمدة لا تتجاوز سنتين وبغرامة لا تتجاوز 5000 ر.ع أو بإحدى هاتين العقوبتين كل من: 3- دخل بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الالكترونية. وهو ما يستفاد منه أن المشرع العماني قد تناول ايضاً جريمة التعدي علي التوقيع الالكتروني ، ولكنه لم يبين على وجه التحديد مفهوم العبث بالتوقيع الالكتروني ، ولعله ترك هذه المحكمة للقضاء ورجال الفقه.

المبحث الثاني
جريمة تزوير التوقيع الإلكتروني

يلاحظ أن **القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** فرق بين عقوبة التزوير في المحرر الإلكتروني الرسمي والإلكتروني العرفي ، حيث **جاء نص المادة (4)** من القانون سالف البيان أنه " يعاقب بالسجن المؤقت كل من

زور مستنداً من مستندات الحكومة الاتحادية أو المحلية ، وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من مستندات إذا كان من شأن ذلك إحداث ضرر.

ويلاحظ أن **القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** لم يفرق بين التزوير العمدي وغير العمدي في معلومات التوقيع الالكتروني ، وعلى ذلك يكون التطبيق وفق القواعد العامة أن الأصل في جريمة تزوير التوقيع الإلكتروني أن تكون عمدية ما لم ينص القانون على غير ذلك.

أولاً - تعريف التزوير المعلوماتي:

التزوير بوجه عام هو "تغيير الحقيقة أيا كانت وسيلته وأياً كان موضوعه". وهو بهذا المدلول يتسع للعديد من الجرائم ، أما التزوير في المحررات فهو حسب تعريفه المستقر في الفقه الفرنسي والمصري "تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون ، تغييراً من شأنه إحداث ضرر مقترن بنية استعمال المحرر المزور فيما أعد له" [1].

ويقصد بالتزوير المعلوماتي "أي تعبير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة او كانت مرسومة عن طريق الراسم ، و يستوي في المحرر المعلوماتي ان يكون مدونا باللغة العربية او لغة أخرى لها دلالتها ، كذلك قد يتم في مخرجات غير ورقية شرط ان يكون المحرر المعلوماتي ذا أثر في اثبات حق او اثر قانوني معين".

ومفهوم ما سبق أن التزوير المعلوماتي يرد على وثائق معلوماتية – حتى ولو كانت محررات باطلة من حيث الشكل – [2] وهي تلك الوثائق التي يتم الحصول عليها بوسائل

1- محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، 1986 ، ص193.

2- من المقرر – في قضاء الاتحادية العليا – أن التزوير في الأوراق الرسمية يعاقب عليه ولو كان حاصلا في محرر باطل شكلاً لاحتمال حصول الضرر منه للغير أو للجميع ، إذ إن المحرر الباطل وإن جرده

معلوماتية ، أي تكون ناشئة عن جهاز الكتروني كهرومغناطيسي أو طبع ممغنط. وان كان هناك في الفقه من يرى عدم الخلط بين الوثائق المبرمجة والوثـائق المعلوماتيـة فالوثيقـة المعلوماتية هي وثيقة لم تبرمج بعد. كذلك توجد جهات يرخص لها سواء كانت شخصية أو اعتبارية ، باعتماد التوقيعات الإلكترونية ، بشهادات مصدق عليها منهم ، وهذه الشـهادات يترتب عليها آثار قانونية تتمثل في انشاء التزامات واثبات حقوق بالنسبة لطرفي العقد فـي التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما.

ثانياً - أركان جريمة تزوير التوقيع الإلكتروني:

التزوير المعلوماتي يتكون من خلق أو تعديل غير مصرح للبيانات المسجلة بطريقة تجعلها تحوز قوة وحجية ، بما يؤدي إلى خداع للحقوق القانونية المحمية وهي أمن وسلامة وإمكانية تشغيل البيانات الإلكترونية. كما وأن الإدخال غير المصرح به للبيانات الصحيحة وغير الصحيحة يخلق موقفاً يناظر عمل محرر مزور ، وأيضا للعمليات اللاحقة للإتلاف كالتعديلات والمحو كواقعة خروج البيانات الممثلة على دعامة والطمس كواقعة حفظ وإخفاء بيانات كل ذلك يوازي تزوير محرر صحيح ، هذا ولقد اشترط القصد الجنائي العام وهو علم الجاني بأنه يقوم بإتلاف أو تعييب توقيع إلكتروني أو وسيط إلكتروني أو تزويرهما مع انصراف إرادته لارتكاب ذلك الفعل.

1- الركن المادي لجريمة تزوير التوقيع الإلكتروني:

الركن المادي لهذه الجريمة يدور حول فعل التزوير أو التقليد الإلكتروني المعلوماتي. مفاد ما سبق أن التزوير المعلوماتي ينصب على تغيير الحقيقة في محرر إلكتروني بطريق الغش ، مما ينتج عنه مضمون مختلف للمحرر وللمعاملات القانونية القائمة علـى صـحة المعلومات التي توفرها هذه البيانات التي تكون محلاً للغش ، ويكون مـن شـأنه إحـداث

القانون من كل أثر فإنه تتعلق به ثقة الغير ممن لا يتضح أمامهم ما يشوبه من عيوب ويصح أن ينخدع به كثير من الناس الذين يفوقهم ملاحظة ما فيه من نقص ، وهذا وحده كاف لتوقيع حصول الضرر بالغير بسبب هذا المحرر ومن ثم فإن ما يثيره الطاعن في هذا الشأن لا يكون مقبولاً. الطعن رقم 4163 سنة قضائية 26 جلسة 2003/4/2.

ضرر[1] ، ولا يُشترط أن يكون التغير كلياً ، أي إبدال كل البيانات بما يخالف الحقيقة ، بل يكفي أن يكون تغيير الحقيقة جزئياً أو نسبياً. ومن أشهر الوسائل التي يمكن الاعتماد عليها في تقليد أو تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتيـة خاصـة بذلك ، يتم تصميمها علي غرار البرامج والأنظمة المشروعة أو محاولـة الـبعض كسـر الشفرة والوصول إلي الأرقام الخاصة بالتوقيع الإلكتروني ، والقيـام بنسـخها ، وإعـادة استخدامها بعد ذلك.

2- الركن المعنوي لجريمة تزوير التوقيع الإلكتروني:

جريمة تزوير التوقيع الإلكتروني تعد من الجرائم العمدية ، صورة الركن المعنوي فيها القصد الجنائي العام بعنصرية العلم والإرادة فيجب أن يعلم الجاني أن التوقيع الإلكتروني أو المحرر الإلكتروني أو الوسيط الإلكتروني مزوراً ، ومع ذلك تتجه إرادته الي الفعل المجرم ويقبل النتيجة المترتبة عليها. وعقوبة هذه الجريمة ، وفقاً لنص المادة (4) مـن **القـانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومـات** ، هـي السـجن المؤقت إذا وقع التزوير على توقيع إلكتروني حكومي رسمي ، وتكـون العقوبـة الحـبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير في معلومات توقيع إلكتروني عرفي.

ثالثاً – صعوبة تزوير التوقيع الإلكتروني:

يتكون التوقيع الإلكتروني إذن من مفتاحين عام وخاص ، أما المفتاح العام فيتم الإعلان عنه في شهادة التصديق على التوقيع الإلكتروني الصادرة من جهة مختصة ، وهو مفتـاح يخص الموقع وحده دون غيره لكنه ينشر لكل ذي شأن ، فالمفتاح العام بمثابة بطاقة إثبات هوية للموقع. وأما المفتاح الخاص فهو عبارة عن مجموعة من البيانات يستأثر الموقع وحده بحيازتها ، ويعتبر بمثابة قلم التوقيع الذي يقوم الموقع من خلاله بتكوين بيانـات توقيعـه ، وهذا يفترض أن يعرض الموقع كيفية استخدامه. ولذلك يلزم لتزوير التوقيع الإلكتروني أن

1- والضرر هو "إهدار حق ، أي إخلال بمصلحة مشروعة ، ومن ثم يعترف بها القانون ويكفل لها حمايته".
- د. محمود نجيب حسني ، المرجع السابق ، ص251.

يستخدم المزور نفس قلم الموقع (المفتاح الخاص) ، ويلزم أيضاً أن يعرف بيانات التوقيع الإلكتروني نفسه (الرقم السري) بالإضافة إلى بيانات المفتاح العام ، وهو أمر غير متاح إلا للموقع دون غيره.

ومن هذا يتضح أن تزوير التوقيع التقليدي أسهل بكثير من تزوير التوقيع الإلكتروني[1] ، حيث إن التوقيع التقليدي يراه الجميع ولا يشترط لتكوينه قلم من نوع خاص ، وهاتان الخاصيتان تميزان التوقيع الإلكتروني ، كما يمكن أيضاً زيادة قيد آخر للتوقيع الإلكتروني يضمن صحة وهو ألا يفتح المفتاح الخاص إلا بعد تكويده بكود معين ، فيكون هناك ثلاثة قيود يجب تجاوزها لتكوين التوقيع الإلكتروني ، أولها بيانات المفتاح الخاص ، وثانيها بيانات التوقيع الإلكتروني (الرقم السري) ، وثالثها كود سري لفتح المفتاح الخاص ، وبذلك يكون التوقيع الإلكتروني معبراً عن هوية الموقع ، لأنه هو وحده الذي يملك أدوات وآليات هذا التوقيع.

رابعاً – جريمة تزوير التوقيع الإلكتروني في التشريع الفرنسي والمصري:

حرص كل من المشرع الفرنسي والمصري على حماية المحرر الإلكتروني الموقع إلكترونياً من مخاطر التزوير التي تهدده في إطار البيئة الالكترونية التي يجري في فلكها ، فقد حرصا على النص على تجريم التزوير الذي يقع على هذه المحررات. غير أن هناك تبايناً في خطة كل منهما في شأن موضع النص على هذه الجريمة ، فبينما يذهب المشرع الفرنسي إلى تجريم تزوير التوقيع والمحررات الإلكترونية عن طريق تبنيه تعديلاً تشريعياً على نصوص التزوير في قانون العقوبات على نحو يسمح بامتدادها إلى الكتابة والمحررات الإلكترونية ، نجد أن المشرع المصري حرص على تجريم تزوير التوقيع والمحررات الإلكترونية بنصوص خاصة في قانون التوقيع الإلكتروني رقم 15 لسنة 2004 (المادتان 23 ، 24). وسنتناول فيما يلي خطة كل من المشرعين الفرنسي والمصري في هذا الشأن.

1- د. محمد المرسي زهرة ، حجية التوقيع الإلكتروني في الإثبات ، بحث منشور بمجلة اتحاد المصارف العربية ، 1991 ، ص 114.

(أ) جريمة تزوير التوقيع الإلكتروني في التشريع الفرنسي:

حرص المشرع الفرنسي مع إصدار قانون العقوبات الجديد عام 1992 وصـــيرورته نافذاً في عام 1994 على تعديل نص جريمة التزوير الوارد في المادة 441-1 من القانون المذكور حتى يمتد مدلول التزوير ليستوعب المحررات الإلكترونية إلى جانب المحـــررات الورقية ، وقد جاءت تلك المادة بتعريف واسع للتزوير Le faux بأنه " كل تغيير بطريـــق الغش في الحقيقة ويكون من شأنه إحداث ضرر ، ويُرتكب بأي طريقة ، سواء أكان ذلـــك بالكتابة أو بأي إفصاح آخر للتعبير عن الفكر الذي يكون الغرض منه أو كنتيجة له شأناً في إثبات حق أو واقعة لها آثار قانونية " [1].

وقد جاءت صياغة المادة 441-1 من قانون العقوبات لتُعدِّل ما كان ينص عليه قانون Godfrain سنة 1988[2] الذي كان يتضمن تجريم تزوير المحررات الإلكترونية أياً كـــان شكلها وذلك متى كان من شأنها الإضرار بالغير (المادة 462-5) ، كما امتد التجريم إلـــى استعمال المحررات الالكترونية المزورة ، وبذلك فإن المشرع الفرنسي فضّل تعديل النص العام في التزوير لكي ينسحب على تزوير المحررات الإلكترونية وذلك بتعديله في مفهـــوم

1- "Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques".

2- القانون رقم 19-88 الصادر في 5 يناير سنة 1988 ، وقد عُرف هذا القانون باسم النائب الفرنسي Jacques GODFRAIN والذي تقدم في 5 أغسطس سنة 1986 باقتراح يرمى إلى إدخال بعض التعديلات على جريمة التزوير في المحررات المنصوص عليها في قانون العقوبات لتشمل أيضاً تغيير الحقيقية في البيانات الإلكترونية ، غير أن هذا الاقتراح لم يؤخذ به ورأى مجلس الشيوخ اعتبار تزوير المحررات الإلكترونية جريمة مستقلة عن جريمة التزوير في المحررات. في هذا الخصوص ، انظر: على عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة فى الفترة من 1-3 مايو 2000 ، المجلد الثانى ، ط3 ، 2004 ، ص39 وما بعدها.

المحرر لكي يتضمن هذه المحررات [1].

ويُستفاد من نص المادة المشار إليها ، أن صياغتها تسمح باستيعاب النص لكل صور التعبير عن الفكر التي تكون في شكل إلكتروني ، بل وحتى تلك التي لم يتوصل إليها العلم بعد ، متى كان لها شأن في إثبات حق أو واقعة لها نتائج قانونية ، كما يتضح منه أيضاً أن المشرع الفرنسي لم يقصر طرق التغيير في الحقيقة على طرق محددة على سبيل الحصر ، وإنما أطلق النص من أي قيد يحدد كيفية وقوع التزوير من خلال تبنيه صياغة مرنة يمكنها استيعاب كافة صور التزوير.

وإذا كان قوام الركن المادي في جريمة تزوير المحرر الإلكتروني هو تغيير الحقيقة ، فإن المشرع الفرنسي وإن حاول أن يعطي مرونة كبيرة في تحديد الركن المادي بقوله إن التزوير هو تغيير الحقيقة ، فإن ما نص عليه هو أقرب للوصف منه إلى تحديد الفعل الذي يقوم به التزوير ، ذلك أن فعل اصطناع المحرر لا ينطوي على تغيير الحقيقة في محرر قائم ، وإنما قد يكون المحرر الذي اصطنعه الجاني ليس له نظير في الواقع [2].

ومن الأهمية بمكان الإشارة إلى أن المشرع الفرنسي تطلب أن يكون من شأن التزوير في المحررات الإلكترونية إحداث ضرر بالغير سواء كان ضرراً قائماً أو محتملاً [3] ، ويكون الغرض منه ، أو كنتيجة له ، شأناً في إثبات حق أو واقعة لها آثار قانونية [4] ، كما تطلب المشرع أن يقع التزوير بطريق "الغش" وأن يكون غرض الجاني من التزوير التأثير

1- لمزيد من التفصيل ، انظر: أشرف توفيق شمس الدين ، الحماية الجنائية للمستند الالكتروني ، دار النهضة العربية ، 2006 ، ص109؛ مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دراسة مقارنة ، دار النهضة العربية ،2001 ، ص30.

2- ومثال ذلك: «أن من يرسل رسالة إلكترونية مصطنعة تتضمن إيجاباً غير صحيح منسوباً لآخر لا يعد تغييراً للحقيقة ، بل الأدنى إلى الصواب هو القول بأنه بيان غير صحيح أيا كانت طريقة تحققه».
– د. أشرف توفيق شمس الدين ، مرجع سابق ، ص113.

3- Cass. crim., 2 Juillet 1980, Bull. Crim. no 210.

4- Cass. crim. 3 mai 1995, Gaz. Pal. 1995, 2, chron. 437, obs. DOUCET.

في إثبات حق أو واقعة لها آثار قانونية.

(ب) جريمة تزوير التوقيع الإلكتروني في التشريع المصري:

وعلى خلاف مسلك المشرع الفرنسي الذي وضع نصوصاً عامة لتجريم التزوير من خلال تعديل نصوص التزوير في قانون العقوبات على نحو يمتد ليشمل التزوير الحاصل في المحررات الإلكترونية ، اتجه المشرع المصري صوب تجريم الصور المختلفة للمساس بالمحرر الإلكتروني ومن بينها جريمة التزوير ، ولكنه أفرد لها نصوصاً خاصة في قانون التوقيع الإلكتروني رقم 15 لسنة 2004 تضمنتها المادتان 23 ، 24 منه دون أي تطرق لنصوص التزوير الواردة في قانون العقوبات.

تقرر المادة 23 من قانون التوقيع الإلكتروني أنه «مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر ، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :....

(ب) أتلف أو عيَّب توقيعاً أو وسيطاً أو محرراً إلكترونياً ، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر.

(ج) استعمل توقيعاً أو وسيطاً أو محرراً معيباً أو مزوراً مع علمه بذلك...».

وفي ذات الاتجاه ، يعاقب المشرع في المادة 24 من القانون المذكور المسؤول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون ، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك.

ويبين من نص المادة 23 من قانون التوقيع الإلكتروني أن المشرع المصرى لم يحدد صور التزوير في المحرر الإلكتروني على سبيل الحصر؛ حيث ينص على وقوعه بطريق "الاصطناع أو التعديل أو التحوير أو بأي طريق آخر" ، وهو ما يُفسح المجال أمام إمكانية الاعتداد بطرق أخرى للتزوير. ولقد أحسن المشرع صنعاً ، بعدم النص في المادة 23/ب

من القانون رقم 15 لسنة 2004 على طرق محددة للتزوير ، حيث إنه أورد الاصطناع والتحوير والتعديل على سبيل المثال كطرق للتزوير ثم نص على التزوير بأي طريق آخر وبذلك لم يحدد طرقاً للتزوير على سبيل الحصر. ذلك أن عدم التحديد لطرق التزوير أمر يضفي – **في اعتقادنا** – على هذا النص طابع المرونة وعدم الجمود في مواجهة ما قد يُسفر عنه التطور من أساليب وطرق للتزوير.

كذلك توجد جهات يُرخص لها سواء كانت شخصية أو اعتبارية ، باعتماد التوقيعات الإلكترونية ، بشهادات مصدق عليها منهم ، وهذه الشهادات يترتب عليها آثار قانونية تتمثل في إنشاء التزامات وإثبات حقوق بالنسبة لطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما. ولذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته. ومن أشهر الوسائل التي يمكن الاعتماد عليها في تقليد أو تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك ، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني ، والقيام بنسخها ، وإعادة استخدامها بعد ذلك.

والجريمة السابقة تعد من الجرائم العمدية ، وصورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة ، حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات ، ومع ذلك تتجه إرادته إلى الفعل المجرم ويقبل النتيجة المترتبة عليها.

خامساً – جريمة استعمال مستند مزيل بتوقيع الإلكتروني مزور مع العلم بذلك:

أضاف **القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** جريمة أخرى ترتبط بالجريمة سابقة الذكر وهي استعمال محرر إلكتروني مزور ، مساوياً في ذلك مسلك قانون العقوبات بإلحاق جريمة استعمال محرر مزور بجريمة التزوير مع تأكيد رغبته في مساواة المحررات والتوقيعات الإلكترونية بالمحررات الورقية والتوقيعات التي تتم على الورق. ويقصد باستعمال التوقيع الإلكتروني المزور أو المعيب إبرازه

والاحتجاج به فيما زور من أجله وذلك على اعتبار أنه صحيح. وهذه الجريمة مستقلة عن جريمة التزوير وتقوم على أركان ثلاثة هي: فعل الاستعمال ، ومحل يقع عليه هذا الفعل وهو التوقيع الإلكتروني المزور أو الوسيط الإلكتروني المزور أو المحرر الإلكتروني المزور ، ثم القصد الجنائي [1].

ويلاحظ أن **القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات** أضاف ركن القصد الجنائي في ذلك الفعل مقرراً مع علمه بذلك ، وهو ما يدل علي وجوب علم الجاني بأنه يقوم باستعمال توقيع أو وسيط الكتروني مزور أو معيب وذلك بغرض إضفاء مزيد من الحماية علي الوسائط الإلكترونية. ويفترض فعل استعمال التوقيع الإلكتروني المزور بطريق الاصطناع أو التحوير أو التعديل أو بأي طريق آخر قيام الجاني باستعمال هذا التوقيع أو المحرر المزور في معاملة من المعاملات ، ولا يشترط أن يحدث استعمال المحرر الإلكتروني المزور ممن قام بتزويره ، وإنما يكفى لقيام الجريمة مجرد استعمال المحرر من جانب أي شخص طالما كان عالماً بطبيعته المزورة وأقدم على استعماله على الرغم من ذلك [2].

وعلى ذلك إذا ما تحقق فعل الاستعمال فيما أعد التوقيع الإلكتروني لأجله ، قامت جريمة استعمال التوقيع الإلكتروني المزور في حق الجاني وعوقب بعقوبتها طالما أنه يعلم بتزويره ، وانصرفت إرادته إلى فعل الاستعمال ، وهكذا الحال بشأن استعمال محرر أو وسيط إلكتروني مزور. وطبقاً للقواعد العامة فإن جريمة استعمال الورقة

1- د. عمر السعيد رمضان ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، 1986 ، ص22.

2- وإلى جانب السلوك الإجرامي في الجريمة المذكورة المتمثل في استعمال المحرر أو التوقيع الإلكتروني المزور ، فإن المشرع المصرى يشترط لقيام الجريمة في حق الجاني توافر الركن المعنوي في صورة القصد الجنائي العام؛ حيث اشترط علم الجاني بحقيقة المحرر أو التوقيع المزور ، ومع ذلك انصرفت إرادته إلى فعل الاستعمال المجرَّم وقبوله النتائج المترتبة على ذلك. انظر: عبد الفتاح بيومي حجازي ، التوقيع الإلكتروني في النظم القانونية المقارنة ، دار الفكر الجامعي ، 2008 ، ص546.

المزورة جريمة مستمرة تبدأ من تقديم الورقة والتمسك بها وتظل مستمرة ما بقي مقدمها متمسكاً بها ، ولا تبدأ مدة سقوط الدعوى إلا من تاريخ الحكم بتزويرها.

المبحث الثالث
جريمة الدخول غير المصرح به
على قاعدة بيانات خاصة بالتوقيع الإلكتروني

قد تتعرض كثير من الأنظمة المعلوماتية للتوقيع الالكتروني إلى الاختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها ، وقد أطلق على هؤلاء الذين يدخلون إلى أنظمة الكمبيوتر بدون تصريح بالقراصنة Hackers. وتختلف الأهداف المباشرة للاختراقات ، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة ، وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه ، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الاختراقيه" ، أو لإثبات وجود ثغرات في الجهاز المخترق. ومن أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت ، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع Defacing ، إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة ، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة. أن التعرض لمفهوم الدخول غير مصرح به Illegal Access إلى النظام المعلوماتي يتطلب بيان ماهية الاختراق وأشكاله على نحو ما يلي.

أولاً - ماهية الدخول غير المصرح به إلى النظام المعلوماتي للتوقيع الالكتروني:

يقتضي تناول ماهية الدخول أو الولوج غير المصرح به إلى النظام المعلوماتي أن نعرض أولاً لمفهوم الدخول:

(أ) – مفهوم الدخول غير المصرح به إلى النظام المعلوماتي:

ينصرف معنى مصطلح " الدخول " access في إطار المعلوماتية بصفة عامة ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي ، ويقصد بالدخول غير المصرح به إلى النظام UNAUTHORIZED ACCESS أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية CONFIDENTIALITY ، أو المساس بالسلامة والمحتوى والتكاملية INTEGRITY ، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها AVAILABILITY.

والاختراق هو " عبارة عن عملية دخول غير مصرّح به إلى أجهزة الغير وشبكاتهم الإلكترونية ، ويتمّ هذا الاختراق بواسطة برامج متطوّرة يستخدمها كلّ من يملك خبرة في استعمالها".

ويتحقق الدخول غير المصرح به إلى جهاز الكمبيوتر بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الكمبيوتر والقوائم والمعدات والمكونات دون رضاء المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها ، أو بمعنى آخر إساءة استخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله لاستخدامها في غرض ما.

وقد جاء نص المادة (2) من قانون الاتحاد الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على أنه " كل فعل عمدي يتوصل بغير وجه حق إلى موقع او نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب عليه بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين".

ويلاحظ أن تحديد فكرة الدخول غير المشروع من حيث دلالة المكان يمكن أن تعرف بأنها " التسلل في داخل النظم المعلوماتية ، أما الدخول من حيث الزمان فيتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز

هذه الفترة الزمنية ، كذلك قد يتحدد مضمون الدخول من زاوية فنية بحيث قد يتم الدخول بصور مختلفة منها الاعتداء على البرامج أو البيانات أو المكونات المادية وقد يتم الدخول بواسطة الغش المعلوماتي ، والذي لا يتطلب تدخلاً في الوظائف الطبيعية للكمبيوتر بإدارة إلكترونية مصطنعة وبالتالي يتم التقاط معلومات أو التنصت عليها. ويختلف فعل الدخول غير المشروع عن فعل البقاء داخل النظام المعلوماتي الذي يعرفه البعض بأنه "التواجد داخل نظام المعالجة الآلية للبيانات ضد إرادة من له الحق في السيطرة على هذا النظام".

(ب) اختلاف جريمة الدخول عن جريمة التخريب العمدي للنظام المعلوماتي:

إذا كان فعل الولوج غير القانوني للنظام المعلوماتي قد اعتبر جريمة وفقاً لاتفاقية بودابست وغالبية القوانين الوطنية ، فإن المجرم المعلوماتي قد لا يكتفي بمجرد الدخول للنظام المعلوماتي ، بل يتعدى هذا الفعل ويرتكب جريمة أخرى وهي تخريب أو إعاقة النظام المعلوماتي.

وفي هذا الصد نجد أن اتفاقية بودابست لسنة 2001 نصت على جريمة المساس بسلامة النظام المعلوماتي في المادة (5) وعنوانها تداخل النظم System Interference والتي جاء نصها علي أنه " يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من التدابير الأخرى يرى أنها ضرورية طبقاً لقانونه الداخلي لاعتبار الأفعال التالية جرائم مؤثمة إذا ما ارتكبت عمداً ، وبدون وجه حق الإعاقة الجدية الخطيرة لوظيفة نظام الكمبيوتر ، عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية ".

وجديراً بالذكر أن الغاية من تلك المادة هي تجريم التخريب والإعاقة Hindering العمدية لنظم المعلوماتية ، إذا ما أدى هذا التخريب إلى إعاقة حسن تشغيل النظم المعلوماتية وفعل الإعاقة المشار إليه في هذه المادة يقصد به الأفعال التي تحمل اعتداء على النظام المعلوماتي بواسطة الإدخال أو الإرسال أو الإتلاف أو الحذف أو التعديل للبيانات المعلوماتية. وقد ارتأى واضعو المعاهدة أن من أمثلة الإعاقة الجسيمة للنظام المعلوماتي إرسال بيانات لنظام معلوماتي معين بشكل وبحجم أو بذبذبة لها أثر ضار على قدرة مالك

النظام أو مشغله على استخدام النظام أو الاتصال بالغير ، ومن أمثلة ذلك إرسال أو زرع فيروسات تؤدي إلى تعطيل أو إبطاء سير النظام المعلوماتي ، وكذلك البرامج التي توجه كميات هائلة من البريد الإلكتروني Spamming إلى المرسل إليه بهدف شل أو تعطيل النظام المعلوماتي.

ويشير نص المادة (5) أيضاً إلى أن الإعاقة يجب ان تكون بدون وجه حق ، بحيث إن الأمر يتعلق بأنشطة اختبار امن نظام الكمبيوتر أو حماية النظام والمصرح بها من المالك أو القائم بتشغيله ، أو عند إعادة تشغيله ، والذي يحدث غالباً عندما يشتري مشغل النظام برنامج كمبيوتر جديداً software ، فكل هذه الأنشطة تعتبر شرعية ، وبالتالي لا يعاقب عليها في ضوء هذه المادة.

(ج) وسائل الاختراق والدخول غير المصرح به للنظام المعلوماتي للتوقيع الالكتروني:

تختلف الوسائل التي يمكن اللجوء إليها للدخول غير المصرح به إلى نظام الكمبيوتر ، ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الكمبيوتر أو فتح البرنامج الذي يقوم بتشغيله ، وقد يتطلب الحصول على الشفرات الخاصة بالدخول باستخدام جهاز لفك الشفرة ، كما يمكن الدخول عن طريق وسائل أخرى للدخول لأنظمة الحاسبات الآلية تعتمد على ضعف الأنظمة ذاتها أو على بعض الأخطاء الناجمة عن عملية البرمجة.

أن غالبية محاولات اختراقات النظم المعلوماتية تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير ، وهنا تكمن الخطورة ، ويلاحظ أن الاختراق لا يطال أجهزة الكمبيوتر إلاّ إذا كانت موصولة بشبكة الإنترنت التي توصل الجهاز بقراصنة الإنترنت. ويعتبر من ضمن جرائم الاختراق أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إما مجرداً أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات Disorderly Persons Offense و Aggravated Computer Trespass و Computer Trespass ، وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب

الكمبيوتر Computer Vandalism وإيذاء الكمبيوترComputer Mischief ، واغتصاب الملكية extortion ، وخلق البرمجيات الخبيثة والضارة Creation of Harmful Programs ، ونقلها عبر النظم وشبكات الاتصالات Transmission of Harmful Programs ، واستخدام اسم النطاق أو العلامة التجارية ، أو اسم الغير دون ترخيص Cyber Squatting ، وإدخال بيانات خاطئة أو مزورة إلى نظام كمبيوتر ، والإتلاف غير المصرح به لنظم الكمبيوتر.

(د) أسباب الاختراق والدخول غير المصرح به للنظام المعلوماتي للتوقيع الالكتروني:

تختلف أسباب الاختراق والدخول للنظام المعلوماتي باختلاف أهداف المخترِق ، فقد يكون الهدف من عملية اخترق أجهزة كمبيوتر البعض أو مواقعهم على الشبكة لمجرّد الفضول ، وقد يخترق بغرض سرقة المعلومات والبيانات ، وهذا هو السبب الأبرز الذي يدفع قراصنة الإنترنت إلى الدخول إلى مواقع وأجهزة كمبيوتر الغير لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل بدل مالي للاضطلاع عليها ، وقد يكون الاختراق في نيّة المخترق في تغيير أو تحريف أو تعطيل المعلومات في أجهزة الغير.

وقد يكون الاختراق تزوير بيانات ومعلومات التوقيع الالكتروني ، وفي هذا الصدد **نصت المادة (4) من قانون الاتحاد الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفا به قانونا في نظام معلوماتي".**

وقد يكون الاختراق بهدف تعطيل الأجهزة والشبكات الخاصة بتشغيل التوقيع الالكتروني ، حيث يتم تعطيل أجهزة الكمبيوتر عبر تعطيل برامجها ، كما قد يؤدي تعطيل البرامج إلى أعطال فنّية تطال قطع الجهاز الإلكترونية ، والهدف من التعطيل هو منع الحواسب والشبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة ، تتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى

الأجهزة أو الشبكات المراد تعطيلها ، الأمر الذي يعيقها عن تأدية عملها ، فقد وقعت بعض المواقع الكبرى المستضيفة للمواقع على الشبكة ضحية هذا التعطيل.

وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومـات المخزنـة داخله بهدف السيطرة على النظام دون تصريح ، أو المساس بسـلامة وأمـن المعلومـات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الإجرامية تتضمن ابتداء الدخول غير المصرح به إلى النظام المعلوماتي.

ثانياً - اختلاف فعل الدخول للنظام المعلوماتي عن غيره من الأفعال المشابهة:

1- اختلاف الدخول عن اعتراض الرسائل المرسلة بطريقة الكمبيوتر :

يختلف اعتراض الرسائل المكتوبة والتي ترسل بطريقة الكمبيوتر سواء بين جهـازين عن طريق شبكة مغلقة أو بطريق شبكة الانترنت عن التداخل ، فـالاعتراض لا يتضـمن تداخلاً في نظام معين ينتمي إلى كمبيوتر معين ، ولكنه يتمثل في التلصص على الرسـائل مثل القانون الانجليزي.

وتقوم عن طريق وضع وسائل سلكية تتصل بالنظام المعلوماتي أو عن طريق التقـاط الرسائل بوسائل التقاط حديثة وذلك عن بعد ، وما دام هذا التلصص لا يتمثل في التداخل في نظام كمبيوتر معين فهو أذن لا يدخل في عداد النشاط الذي تعاقب عليه بعـض القـوانين بوصفه تداخلا ، كما أنه لا يعتبر معاقباً عليه بوصف التنصت على المحادثات التي تجري في مكان خاص والذي تعرفه غالبية القوانين ، ومن هنا كان واجبا إيراد نص خاص يعاقب على التنصت على النظام.

2- اختلاف الدخول في النظام المعلوماتي عن استعماله:

تختلف فكرة الدخول عن استعمال النظام ، وبالتالي فإن المشعر إذا جرم الدخول فـإن ذلك لا يعني ان يقوم الفاعل باستعمال الجهاز ، فدائرة الدخول أضيق من دائرة الاستعمال.

فكل استعمال لنظام دون رضاء صاحبه يشكل دخولا بلا ريب فيه ، أما الــدخول فإنـــه لا يعني بالضرورة استعمال النظام. فقد يتصل الشخص بالنظام ومن ثم يكون قائما بالــدخول فيه ولكنه لا يستعمل إمكانيات النظام ، كأن يكتفي بالاطلاع على النظام بوسائل سلكية (أي اتصال بدوائر سلكية تتصل بالنظام) أو بوسائل غير سلكية أو باستعمال بـــرامج خاصـــة بالاقتحام والفاعل يكتفي عندئذ بالاطلاع دون استعمال النظام.

ثالثاً - طرق الدخول غير القانوني للنظام المعلوماتي للتوقيع الالكتروني:

أن الولوج غير القانوني أو غير المصرح به ، له مجموعة من الصور أهمها ، اختراق النظام كله أو جزء منه ، ويستوي هنا أن يكون الجزء مادياً أو برامج جزئية ، أو بيانـــات مخزنة فى نظام التنصيب Installation ، أو بيانات تتعلق بالمرور أو المحتوى. وتتعـــدد الطرق التي يمكن أن يستخدمها المجرم المعلوماتي للدخول للنظـــام المعلومـــاتي ومنهـــا : تشغيل كمبيوتر مقفول ، أو مفتوح ، أو عن طريق استعمال كـــارت تشـــغيل أو بواســـطة استعمال خط تليفوني ، أو من خلال الدخول إلي كمبيوتر من كمبيـــوتر آخـــر ، وكـــذلك بواسطة الدخول الي نظام متصل بنفس الكمبيوتر بدائرة واحدة ، ونتناول ذلك بشـــيء مـــن التفصيل على نحو ما يلي.

1- تشغيل كمبيوتر مغلق:

تتمثل هذه الطريقة في أن المتهم يقوم بفتح جهاز الكمبيوتر وتشغيله بعد أن كان مغلقا ، فإذا ما بدأ العمل فإن المتهم يعتبر قد دخل النظام بدون وجه حق ، طالمـــا تـــم ذلـــك دون موافقة صاحب الحق في ذلك.

ويذهب البعض إلى أن العبرة ليست هي بتشغيل جهاز الكمبيوتر ولكن بـــالتمكن مـــن الدخول إلي الملفات ، اذ قد يتمكن المتهم من الدخول إلي الملفات الموجودة داخل الجهـــاز على الرغم من أن الجهاز مغلق ، كما أنه قد يتمكن من تشغيل الجهاز ، وذلـــك بإيصـــال الكهرباء إليه ، دون أن يتمكن من الدخول إلى الملفات ، عندئذ يعتبـــر نظـــام المعلومـــات المبرمجة مقفلاً على الرغم من أن الجهاز في وضع "on". بيد أنه في الحالة الأخيرة يعتبر

المتهم قد حاول الدخول إلى الجهاز وهو ما تعتبره بعض التشريعات متساوياً في وقوع الجريمة مثل الدخول نفسه ، وإلا فإنه لا مناص من اعتباره شروعاً إذا كان القانون يعاقب علي الشروع في تلك الجنحة بنص خاص. ومن المعلوم أن معظم التشريعات لا تعاقب علي الشروع إلا إذا ورد نص خاص بخصوص جريمة معينة يعاقب فيها المشرع علي الشروع قانوناً.

2- استعمال كمبيوتر مفتوح :

قد يكون جهاز الكمبيوتر قيد الاستعمال ممن له الحق في ذلك ، فإذا تغافل عنه أو انشغل وقام شخص آخر باستعماله وذلك بأن فتح ملفات متواجدة فيه ، فإنه بذلك يكون قد دخل في هذا النظام ويقع منه النشاط المعاقب عليه ، ويختلف هذا الغرض عما لو كان الكمبيوتر قيد الاستعمال واكتفي المتهم بالنظر إلي الملف الذي كان مفتوحاً أمام المستخدم.

3- الدخول إلي كمبيوتر عن طريق استعمال كارت تشغيل ينتمي الى شخص آخر :

قد يتمكن المتهم من الحصول على كارت (بطاقة) للدخول الي كمبيوتر إحدى الجهات لكي يحص على خدمة معينة ذلك إذا كان النظام يسمح بالدخول بدون رقم سري. هذا الدخول إلى النظام عن طريق استعمال بطاقة خاصة بذلك يحدث عادة في حالة سحب مبالغ من البنوك ، تطبيقاً لذلك قضت محكمة باريس بوقوع الجريمة ممن استخدم كارت السحب من ماكينة السحب الآلي مع الرقم السري الخاص بهذا الغير دون موافقته معتبرة ذلك من قبيل الدخول المعاقب عليه في النظام.

4- الدخول إلى كمبيوتر عن طريق خط تليفوني :

قد يتمكن المتهم من الوصول إلى نظام الكمبيوتر عن طريق العبث بالخط التليفوني المربوط عليه هذا النظام ، فيمكنه هذا من الاتصال بنظام من أنظمة الكمبيوتر وعادة ما يقوم المتهم بذلك بغية التوصل إلى أعطاء أوامر لنظام الكمبيوتر لتحقيق غاية معينة ، وقد كان ذلك هو شأن المتهمين الذين يعملون في شركة التليفونات الفرنسية والذين استعملوا خط

التليفون المركب عليه أجهزة عارضة للألعاب الالكترونية وتمكنوا بذلك من الحصول علي جوائز تقدمها الشركة لمن يفوز في هذه الألعاب [1].

5- الدخول إلى كمبيوتر من كمبيوتر آخر :

قد يتمكن المتهم – و هو يستعمل جهاز الكمبيوتر بطريقة قانونيـــة – أن يـــدخل الـــى معلومات في كمبيوتر آخر ، على الرغم من عدم وجود دائرة مشتركة بـــين الجهـــازين ، ويحدث ذلك باستعمال وسائل مختلفة ، منها أجراء توصيله بدون موافقة صـــاحب الجهـــاز الثاني ، ومنها التجسس عن بعد باستعمال وسائل تقنية حديثة (برامج اختراق النظام مـــثلا) ودون إجراء أية توصيلات. وقد يتمكن المتهم من الدخول الى نظـــام آخـــر مـــن أنظمـــة الكمبيوتر بالاتصال عن بعد بهذا النظام والتوصل إلى معرفة كلمة السر والدخول إلى النظام كله أو جزء من ، كل ذلك يتحقق به الفعل المعاقب عليه [2].

ومن التطبيقات علي هذه الصورة من صور النشاط الإجرامي أن يقوم المتهم بالدخول في نظم كمبيوتر معين ليعطيه أمراً بطريقة مشروعة لتحويل مبلغ مالي إلي حساب معـــين. وجديراً بالذكر أن شبكة الإنترنت تسهل استعمال تلك الوسيلة في الدخول في أنظمة الغيـــر التي تتصل بتلك الشبكة ، وفي نفس الوقت تجعل من الصعب تحديد شخصية المتداخل الذي قد يعمد إلى الدخول من جهاز إلي جهاز آخر مروراً بجهاز ثالث ، كما أنه قد يقوم بـــذلك من خارج البلاد ، وتكون الجريمة حينئذ عابرة للحدود.

1- Aix En – Provence , 23 Oct , 1996, Gaz Pal. 1997. 2. 489, Note Laty Bonnart, Rev.Sc.Crim.1998.140,Obs Francillon.

2- Travaux De I'institut De Sciences Criminells De Protiers, Ifomatique Et Droit Penal , Ed. Cujas, 19983, p25.

6- الدخول الى نظام متصل بنفس الكمبيوتر بدائرة واحدة: [1]

يقوم المتهم في هذه الحالة باستعمال جهاز كمبيوتر بطريقة قانونية ، فقد يكون جهازه وقد يكون جهاز شخص آخر يقوم باستعماله بموافقة منه ، لكنه يستعمل هذا الجهاز في الدخول إلي أنظمة ويفترض هذا النشاط المعاقب عليه أن المتهم ليس من حقه الدخول في النظام ، فإذا كان من حقه هذا الدخول فإن الجريمة لا تقع ، حتى ولو قام باستعمال هذا النظام في غير الغرض الذي سمح به صاحبه. وتطبيقا لذلك قضى في إنجلترا (في 14 نوفمبر سنة 1994) بعدم وقوع الجريمة الذي اتصلوا بإحدى الصحف العامة لكي يثبتوا لهم أن أجهزة الكمبيوتر الخاصة بتلك الجهة يمكن اختراقها والاطلاع على أسرار الجمهور لدى تلك الجهة ، وقاموا بإجراء تلك التجربة من خارج تلك الجهة [2].

7- التجسس على النظام بعد اقتحامه: [3]

في هذا الفرض لا يقوم الفاعل باستعمال النظام ، ولكنه يتجسس على النظام ، فإذا اقتصر فعله على الاطلاع عليه من الخارج ، فإن الأمر يقتصر على التجسس فقط دون التداخل ، وهناك وسائل عديدة لهذا التجسس منها وضع توصيلات بالجهاز بدون موافقة صاحبه ، [4] ومنها اتباع وسائل حديثة – كبرامج اختراق – لالتقاط المعلومات التي يحتويها الجهاز عن بعد ويحدث هذا الفرض الأخير عادة عند استعمال الجهاز وليس تركه مغلقاً.

رابعاً - أركان جريمة الدخول غير المصرح به إلى نظام التوقيع الالكتروني:

تتطلب جريمة الولوج غير القانوني للنظام المعلوماتي إلى توافر ركن مادي وركن معنوي بشقيه القصد عام والقصد الخاص ، ونتناولها على نحو ما يلي:

1- شيماء عبد الغني محمد ، رسالة دكتوراه حقوق عين شمس ، الحماية الجنائية للتعاملات الإلكترونية ، 1992 ، ص30 وما بعدها.

2- Cited By : Stanley Lai, Unauthorized Use And Section 1 Of The Computer Misuse Misuse Act 1990",Journal Of Financial Crim, May 1996, Vbol3,No4,P.359.

3- شيماء عبد الغني محمد ، المرجع السابق ، ص35 وما بعدها.

4- Guillaune Champy, La Frade Infomatique, Op.Cit,P.153.

(أ) الركن المادي لجريمة الدخول غير القانوني للنظام المعلوماتي للتوقيع الالكتروني:

تقوم جريمة الدخول غير المصرح به الى نظام الكمبيوتر والمعلومات التي يحتوي عليها ، بفعل الدخول الذي يطلق عليه الدخول المنطقي ، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية. ويختلف المحل الذي يتخذه الركن المادي في جريمة الدخول غير المصرح به الى نظام مواقع الويب web site ، ويتم عادة التفرقة في هذا الخصوص بين العمليات التي تنطوي على اعتراض لعمليات الاتصال من أجل الدخول إلى أحد نظم الكمبيوتر وبين الدخول إلى أحد نظم الكمبيوتر ، وبين الدخول المباشر الى هذه النظم.

ويمكن بالنظر الى التشريعات المختلفة التي جرمت الدخول غير المصرح به الى نظام الكمبيوتر ، أن نميز بين ثلاث صور للمحل في جريمة الدخول غير المصرح به ، فالصورة الأولى : المعلومات فى ذاتها ، والثانية : نظم أجهزة الكمبيوتر التي لا ترتبط فيما بينها من خلال شبكة للاتصال ، والثالثة : شبكات المعلومات ، فقد يتمثل الفعل الذي يكون الركن المادي في الدخول المباشر إلى المعلومات أو النظام ، أو في عملية الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام.

(ب) الركن المعنوي في جريمة الدخول للنظام المعلوماتي للتوقيع الالكتروني:

ويشكل الركن المعنوي أهمية في قيام جريمة الدخول غير المصرح به الى نظام الكمبيوتر ، فالأفعال التي تقوم بها هذه الجريمة يقوم بها كل يوم مستخدمو الكمبيوتر ، ومن بين هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي. فالركن المعنوي لجريمة الدخول غير المصرح به الى نظام الكمبيوتر في كل التشريعات التي تناولناها يتخذ صورة القصد الجنائي ، باعتبارها من الجرائم العمدية ، فلكي يتوافر لهذه الجريمة ركنها المعنوي يجب أن تتحقق عناصر القصد الجنائي من علم وإرادة ، وسوف نتناول فيما يأتي القصد العام المطلوب تحققه في جريمة الدخول غير المصرح به إلى نظام الكمبيوتر ، ثم نتعرض للقصد الخاص في هذه الجريمة.

1- القصد العام في جريمة الدخول غير المشروع للنظام المعلوماتي للتوقيع الالكتروني:

عبرت جميع النصوص القانونية التي تناولت جريمة الدخول غير المصرح بـه إلـى نظام الكمبيوتر عن القصد العام المتطلب في هذه الجريمة ، وذلك على الرغم من الاختلاف في العبارات المستخدمة لهذا الغرض ، فقد عبر النص الفرنسي عن القصد العام بتطلبه أن يكون الدخول الى النظام قد تم عن طريق الغش والخداع ، فاستخدام هذه العبارة يعنـي أن الفاعل على علم بأن دخوله الى نظام الكمبيوتر غير مصرح به.

وفي الدنمارك أشار النص الى ان الفاعل يقوم بالدخول غير المصرح به الى النظـام على نحو مخالف للقانون ، وفي فنلندا وسويسرا والبرتغال والولايات المتحـدة الامريكيـة اشترط أن يتم الدخول الى النظام بدون تصريح ، وفي السويد واليونان أن يتم الدخول الـى النظام بدون وجه حق ، وقد تطلب القانون الانجليزي أن يتم الدخول إلى النظام على نحـو غير مصرح به مع العلم بذلك ، وفي هولندا واستراليا أن يتم الدخول عمداً وعلى نحو غير مشروع أو بدون وجه حق [(1)].

ويتطلب القصد العام ان يحيط علم الجاني بكل واقعة ذات أهمية قانونية فـي تكـوين الجريمة ، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة واستكمال عناصرها يتعين أن يشمله علم الجاني ، ولكن علم الجاني لا يقتصر نطاقه على الوقائع التي تـدخل فـي تكوين الجريمة ، وإنما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقـائع وتكتسب به أهميتها فى نظر القانون [(2)] ، حيث إن عدداً من الوقائع التي تقوم بها الجريمـة لا تمثل أهمية في نظر القانون ، إلا إذا اكتسبت وصفاً معيناً ، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية ولم تعد صالحة لتقوم بها الجريمة.

1- د. نائلة عادل محمد فريد قورة ، رسالة دكتوراه حقوق القاهرة ، 2007 ، ص 379.

2- د. محمود نجيب حسني: النظرية العامة القصد الجنائي – دراسة تأصيلية مقارنة للركن المعنوي فى الجرائم العمدية ، 1988 ، ص51.

ويتطلب القصد الجنائي أيضاً أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التـــي سوف تترتب على الفعل ، فتوقع النتيجة هو الأساس النفسي الذي تقوم عليـــه إرادتهـــا ، فحيث لا يكون التوقع لا تتصوره الإرادة (1) ، والنتيجة التي يجب أن يتجـــه اليهـــا توقـــع الفاعل هي النتيجة التي يحددها القانون ، وهي الدخول غير المصرح به إلى النظـــام. ولا يشترط أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجـــة ، فالقصد الجنائي يتوافر ولو لم يتوقع الجاني هذه الآثار ، فيتعين إذن أن يتوقع الجـــاني أنـــه سوف يدخل الى نظام غير مصرح له بالدخول إليه ، ولا يشترط أن يتوقع الجاني أنه سوف يدخل ذلك نظام غير مصرح له بالدخول إليه ولا يشترط أن يتوقع الضرر الـــذي ســـوف يلحق النظام من جراء هذا الدخول.

ولا تقتصر فكرة القصد الجنائي على العلم بالوقائع فقط بل تتطلب العلم باكتساب بعض هذه الوقائع تكييفا معينا فبعض الجرائم لا تقتصر عناصرها على وقائع مجردة عن التكييف بل يعد التكييف الذي تكتسبه هذه الوقائع من بين عناصرها الأساسية وفي مثل هذه الجرائم يمثل التكييف ذات الأهمية القانونية التي تمثلها الوقائع في ماديتها (2) ، ولما كـــان القصـــد الجنائي يتطلب علما بكل عناصر الجريمة فهو يتطلب حتما انصراف العلم إلى التكييف كما يتطلب إحاطته بالوقائع ، فإذا كان التكييف عنصرا في الجريمة ، إذ بدونـــه ينتفـــي أحـــد أركانها ، وتصبح الواقعة التي تجردت من هذا التكييف غير أهمية قانونيـــة فـــي تكـــوين الجريمة ، فانه ينبغي أن يشمل علم الجاني هذا التكييف كي يتوافر القصد الجنائي.

2- القصد الخاص في جريمة الدخول غير المصرح به:

تتطلب بعض النصوص التي جرمت الدخول غير المصرح به الى نظام الحاسب الآلي في التشريعات المختلفة قصدا خاصا الى جانب القصد العام وقد يترتب على تـــوافر هـــذا القصد تشديد العقوبة ففي الدنمارك تشدد العقوبة متى ارتكب فعل الدخول بنيـــة الإحاطـــة

1- د. محمود نجيب حسني ، المرجع السابق ، ص65.

2- د. محمود نجيب حسني ، المرجع السابق ، ص58.

بمعلومات تتعلق بالأسرار المتعلقة بعمل احدى الشركات ، وفي استراليا يوجد نص خاص يشدد العقوبة متى ارتكب فعل الدخول غير المصرح به الى نظام الحاسب الالى بنية الأضرار بالغير وفي النرويج تشدد العقوبة على نحو ملحوظ متى ارتكب فعل الدخول غير المصرح به بنية حصول الفاعل له أو للغير على ربح غير مشروع او الحاق ضرر بالغير نتيجة للاطلاع على المعلومات التي يحتوى عليها النظام.

وفي المملكة المتحدة يتضمن قانون إساءة استخدام الكمبيوتر لسنة 1990 في مادته الثانية نصاً يجرم الدخول غير المصرح به متى توافر لدى الفاعل قصد خاص يتمثل فى نية ارتكاب جريمة أخرى لاحقة على هذا الدخول ، فإلى جانب المادة الأولى من هذا القانون والتي تجرم الدخول غير المصرح به إلى نظام الكمبيوتر جاءت المادة الثانية بجريمة أخرى عرفت باسم الدخول غير المصرح به الى نظام الكمبيوتر بنية ارتكاب أو تسهيل ارتكاب جرائم أخرى ، وقد جاء نص هذه المادة على أنه "ويتعين لقيام هذه الجريمة أن تتوافر لدى الفاعل نية الدخول الى النظام مع العلم بكون هذا الدخول غير مصرح به وأن تتوافر لديه نية ارتكاب جريمة أخرى" [1].

خامساً - موقف بعض التشريعات الأجنبية من تحديد محل جريمة الدخول غير القانوني للنظام المعلوماتي:

اهتم المشرع في معظم دول العالم بمسألة مواجهة صور الإجرام المعلوماتي ، وعلى الأخص المرتبطة بالاعتداء على نظم المعالجة الآلية للبيانات ، وبالتالي كثرت التشريعات الوطنية الهادفة لحماية هذه النظم المعلوماتية مع فرض عقوبات صارمة ضد المعتدين على المعطيات المعلوماتية.

وقد اختلفت تشريعات الدول في تحديد محل الدخول غير المصرح به إلى نظام الكمبيوتر ، وهي لا تخرج عن ثلاثة اتجاهات:

1- Bainbridge David:Introduction to Computer Law, Fourth Edition, Longman,2000 p314.

الاتجاه الأول: وهو الذي يجمع بين المعلومات وأنظمة الكمبيوتر وشبكات المعلومات ، وهذا الاتجاه الموسع يتسع ليشمل شبكات المعلومات وبالتالي يشمل التجريم عمليات الاعتراض غير المشروعة للاتصالات التي تتم من خلال الدخول إلى هذه الشبكات ، ويعتبر القانون الفرنسي مثالاً يحتذى به في هذا الاتجاه.

الاتجاه الثاني: وهو الاتجاه الذي يستبعد شبكات المعلومات من نطاق التجريم ، ويعتبر القانون الإنجليزي بشأن إساءة استخدام الكمبيوتر لسنة 1990 من أبرز الأمثلة على هذا الاتجاه ، حيث نجد المادة الأولى من هذا القانون تعاقب على الدخول غير المصرح به إلى البرامج والمعلومات التي يحتوي عليها أي كمبيوتر.

الاتجاه الثالث: تجريم الدخول غير المصرح به إلى أنظمة الكمبيوتر عبر شبكات المعلومات ، ووفق القانون السويسري تم إدراج جريمة جديدة تضمنتها المادة 143 مكرر من قانون العقوبات تعاقب على الدخول غير المشروع إلي أنظمة الكمبيوتر بواسطة جهاز لنقل المعلومات [1].

(1) موقف القانون الأمريكي:

بخصوص جرائم الاختراق نظم معالجة البيانات او الاعتداء عليها فقد كان المشرع الامريكي سباقا في تقرير العقاب على هذه النوعية من الجرائم [2] ، فمنذ عام 1984 تم إصدار قانون تزييف آليات الدخول والإساءة والاحتيال عبر الكمبيوتر الذي يعد أول تشريع عالمي في هذا الإطار ، وبالتالي تم اعتبار كل دخول غير مشروع إلى معلومات مصنفة في حاسوب جنحة [3] ، أما إذا كان الدخول غير المشروع قاصداً سجلات مالية أو سجلات

1- د. نائلة عادل محمد فريد ، المرجع السابق ، ص329.

2- أمين أعزان ، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة ، رسالة دكتوراه حقوق عين شمس ، 2005 ، ص92 وما بعدها.

3- USA V.Robert Taooan Morris, No.774, DOCKET 90-1336. United state court of appeals, second circuit, argued dee4, 1990. decided march 7, 1991.928f.2d504 www.loundv.com/e-law

ائتمان في المؤسسات المالية أو انتهاك حرمة كمبيوتر الحكومة الفيدرالية فإن الجريمة تأخذ شكل جناية [1].

وقد عرف هذا القانون الامريكي مجموعة من التعديلات ، كان أولها عام 1986 ، أما التعديل الثاني فكان عام 1994 ثم عام 1996 [2] ، ففي تعديل 1986 قرر المشرع الامريكي – استثناء على ما هو مقرر في المادة 4–أ من القانون 1030 من التقنين الامريكي المتعلق باستخدام الحاسوب – اعتبار مسألة استهلاك وقت الحاسوب انتهاكا يمكن أن يصل الى درجة الاتهام الجدي في هذا الاطار ، كما اعتبر تعديل 1986 ان مثل هذا الانتهاك هو احتيال يمكن ان يكون مرتكبه عرضة للمساءلة بمقتضى المادة 5 (أ) من الفصل 1030 المذكور ، اذا كان انتهاك زمن استخدام الحاسوب قد نتج عنه ضرر عمدى [3].

(2) موقف القانون الفرنسي:

وفي فرنسا صدر قانون 5 يناير 1988 بشأن جرائم الغش المعلوماتي المرتكبة ضد نظم المعلوماتية ، وتضمن هذا القانون عدة مواد منها نص المادة 2/462 والتي تجرم الدخول أو البقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية للبيانات.

1– أمين أعزان ، المرجع السابق ، ص91 وما بعدها.

2- Hether Jacobson –Rebecca Green, Computer Crimes, American criminal law Review, Spring 2002,Number, p279.

3– ونشير الى انه بموجب هذا التعديل تمت محاكمة اشهر مرتكب اول جريمة نشر دودة "worm" عبر الانترنت وهو طالب R.T.Morris الدكتوراه فى علوم الحاسوب بجامعة كورنيل ، ولقد تم اعتبار موريس مرتكبا لجريمة تجاوز الدخول غير المصرح به الى اجهزة كمبيوتر فيدرالية ، وتعتبر هذه الجريمة بمثابة جناية حسب القانون الامريكي المذكور وهي الجريمة الواردة في المادة 5 أ من الفصل 1030 من التقنين الفيدرالي الامريكي ، حيث لم يكن تعديل عام 1986 يعرف جريمة العدوان الفيروسي وهي الجريمة التي تقررت في تعديل عام 1994.

– راجع في ذلك : عمر محمد ابو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت رسالة دكتوراه ، مرجع سابق ، ص318.

وقد جاء نص المادة 2/462 على أن " كل شخص قام بالدخول أو البقاء بطريقة كلياً أو جزئياً في داخل نظام لمعالجة المعلومات سيعاقب بالحبس الذي لا يقل عن شهرين ولا يزيد على خمسين ألف فرنك أو بإحدى هاتين العقوبتين ، وإذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل في المعطيات المختزنة في النظام تكون العقوبة الحبس لمدة تتراوح ما بين شهرين إلي سنتين والغرامة التي تتراوح ما بين عشرة آلاف جنيه إلي مائة ألف فرنك.

أما بالنسبة لإفساد Fausser تشغيل نظام المعالجة الآلية للبيانات فهو يؤثر في أداء الأجهزة الإلكترونية والحواسيب ؛ بحيث لا تعمل بصورة معتادة ، على أن ذلك لا يصل إلى حد توقف الأجهزة عن العمل ، ومثال ذلك إرسال شخص لعدد هائل من الرسائل الإلكترونية إلى أحد مواقع الويب مما يؤدى إلى إرباك النظام المعلوماتي وتعطل الموقع [(1)]. وقد أجاز المشرع الفرنسي بموجب المادة 6/323 ، وبغرض حماية نظم المعلومات ، مسألة الأشخاص الاعتبارية عن الجرائم المذكورة سلفاً في ضوء الأحكام العامة لمساءلة الأشخاص الاعتبارية الواردة بالمادة 2/121 من قانون العقوبات.

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام ، وبالتالي يجوز الدخول إلى النظام بأية وسيلة ، مثل الدخول عن طريق كلمة السر الحقيقية عندما يكون الجاني غير مخول له استخدامها ، أو استخدامها برامج أو شفرة خاصة ، أو عن طريق استخدام الرقم الكودي لشخص آخر ، أو الدخول من خلال شخص مسموح له بالدخول ، سواء تم ذلك عن طريق شبكات الاتصال التليفونية ، أو محطات طرفية Terminal سواء محلية أو عالمية [(2)].

كذلك من صور الدخول غير المشروع ، أن يكون مالك النظام قد وضع قيوداً للدخول إلى النظام ولم يلتزم الجاني هذه القيود ، أو كان الأمر يتطلب سداد مبلغ نقدي لم يسدده

1- جميل عبد الباقى الصغير ، الإنترنت والقانون الجنائي ، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، سنة 2001 ، ص63.

2- أمين أعزان ، المرجع السابق ، ص101.

الجاني وقام بالدخول غير المشروع إلى النظام ، ويلاحظ في هـذا الصـدد أن المشـرع الفرنسي يعاقب على الدخول المجرد إلى النظام المعلوماتي ، فمجرد الـدخول تقـوم بـه الجريمة حتى ولو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول نفع أو فائـدة طالما أن الدخول غير مشروع.

ويتحقق فعل الدخول كذلك ، كلما دخل الجاني إلي النظام كله أو جزء منه كال دخـول إلى شبكة الاتصال أو البرنامج ، ويتحقق الدخول غير المشروع كذلك متى كان مسـموحاً للجاني بالدخول لجزء معين في البرنامج حيث تجاوزه إلى جزء آخر غيـر مسـموح لـه بالدخول فيه ، فمثلاً لو أن الجاني دخل على موقع www.amazon.com وهو موقع للبيع الإلكتـروني معد للجمهور ، لكنه تجاوز الموقع إلى البيانـات الخاصـة بإعـداد الموقـع وتنظيمه ، في حين أن هذه البيانات أو المعلومات لا يجوز للجمهور الدخول عليها ، فهنـا يكون فعل الجاني مكوناً لجريمة الدخول غير المشروع رغم أن الموقع مفتوح للجمهور [1].

3- القانون السعودي:

القانون السعودي بشأن مكافحة جرائم المعلوماتية لسنة 2007 ، جرم الـدخول غيـر المشروع بطريقة متعمدة إلى الكمبيوتر ، أو موقع إلكتروني ، أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها ، فقد جاء نص المادة (5) على أنـه "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1- الدخـول غير المشروع لإلغاء بيانات خاصـة ، أو حـذفها ، أو تـدميرها ، أو تسريبها ، أو إتلافها أو تغييرها ، أو إعادة نشرها.
2- إيقاف الشبكة المعلوماتية عن العمل ، أو تعطيلها أو تدمير ، أو مسح البرامج ، أو البيانات الموجودة ، أو المستخدمة فيها ، أو حذفها ، أو تسريبها ، أو إتلافها ، أو تعديلها.

1- د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية ، 2001 ، ص53.

3- إعاقة الوصول إلى الخدمة ، أو تشويشها ، أو تعطيلها ، بأي وسيلة كانت.

سادساً - موقف اتفاقية بودابست لسنة 2001 [1] من جريمة الدخول غير المصرح به داخل النظام المعلوماتي:

نتناول في هذا الصدد موقف اتفاقية بودبست 2001 ، ثم نعرض لموقف التشريعات الوطنية الحديثة وذلك على نحو ما يلي: قامت اللجنة الأوروبية بشأن مشاكل الجريمة وبالتعاون مع لجنة من الخبراء فى مجال جرائم الكمبيوتر بإعداد مشروع اتفاقية دولية تتعلق بجرائم الكمبيوتر ، وقد أعلن المجلس الاوربى مشروع هذه الاتفاقية فى 27 ابريل 2000 [2].

وأكد المجلس الاوربي [3] أن الاعتداءات الحديثة على مواقع الانترنت التجارية مثل : أمازون دوت كوم Amazon.com ودالوز دوت فر Dalloz.fr ، هي التي لفتت نظر المجتمع الدولي إلى المخاطر والتحديات التي تواجهها الشبكة الدولية للمعلومات وشبكات الكمبيوتر ، وأن جرائم الكمبيوتر أصبحت قبل أي وقت مضى تهدد بشكل واضح وخطير التجارة والمصالح الحكومية [4].

وعليه فقد بادر المجلس الاوربى إلى وضع مشروع اتفاقية خاصة بجرائم الكمبيوتر ، مع الأخذ في الاعتبار الطابع الدولي الذي يميز هذه النوعية من الجرائم ، وبعد سنة ونصف تقريباً من المناقشات والتعديلات على هذا المشروع تم التوقيع على اتفاقية بودابست بتاريخ 23 نوفمبر 2001 بشأن الإجرام المعلوماتى [5] ، وذلك أيماناً من الدول الأعضاء في المجلس الاوربى والدول الأخرى الموقعة على هذه الاتفاقية بضرورة مواجهة هذا النمط الجديد من الإجرام.

1- The Budapest International Convention On Cybercrime 2001.

2- يمكن الحصول على هذه الاتفاقية من الموقع: www.cybercrime.gov/coedraft.html

3-Floret latrive:41 pays contre les pirates.disponible sur :www.liberation.com/multi/actu/20000424/20000427chtml

4- Convention sur la cybercriminalite, Budapest, 23-11-2001.

5- أمين أعزان ، المرجع السابق ، ص82 وما بعدها.

ونشير فى هذا الصدد إلى أن الانضمام للاتفاقية متاح كذلك للدول غير الأوربية وهـذا ما يوضح الطابع الدولي لهذه الاتفاقية ، ثم أن هذه الأخيرة هي أول اتفاقية يتبناها المجلـس الأوربي وتتسم بالطابع الدولي بالرغم من أن مصدرها أوربي ومن بين الدول غير الأوربية التي وقعت على هذه الاتفاقية نجد الولايات المتحدة الأمريكية وكندا وجنوب أفريقيا. ونشير إلى أن هذه الاتفاقية تتكون من ثمان وأربعين مادة موزعة على أربعة أبواب ، يعالج الباب الأول منها استخدام المصطلحات ، أما الباب الثاني فهو مخصـص للإجـراءات الواجـب اتخاذها على المستوى القومي ، سواء من الناحية الموضوعية أو الإجرائية ، أمـا البـاب الثالث فقد تم تخصيصه للتعاون الدولي ، في حين يتعرض البـاب الرابـع فقـد تعـرض للشروط الختامية.

وبرجوعنا لهذه الاتفاقية المبرمة عام 2001 نجد أن هناك مجموعة مـن المقتضـيات القانونية تصب في إطار حماية النظم المعلوماتيـة ، وبالتـالي حمايـة مواقـع التجـارة الالكترونية بطريقة غير مباشرة ، وتتجلى هذه المقتضيات في المـادتين (2 ،5) ، فالمـادة (2) متعلقة بالولوج غير القانوني للنظام المعلوماتى كما هو الحال بالنسبة لموقـع التجـارة الالكترونية الذي قد يتعرض كأي نظام لجريمة الولوج غير القـانوني ، أمـا المـادة (5) فنجدها تتطرق لمسألة سلامة النظام المعلوماتى ، وبالتالي فهذه المادة تطبق علـى حـالات المس بالبيانات والمعلومات الموجودة داخل الموقع المخصص للتجارة الالكترونية.

وقد نصت اتفاقية بودابست لسنة 2001 بشأن مكافحة جرائم الفضاء المعلوماتي[1] في المادة الثانية [2] منها والمتعلقة بالدخول غير المشروع للنظام المعلوماتي "أن كل طرف (أي الدولة الموقعة) أن يتبنى الاجراءات التشريعية Legislative ، أو اية إجـراءات أخـرى

1- The Budapest International Convention On Cybercrime 2001.

2- Article2- Acces illegal chaque partie adopte les mesures legislatives et autres qui se revelent necessaries pour eriger en infraction penale, conforement a son droit interne l'acces interntionnel et sans droit a tout ou partie d'un systeme informatique. Une partie peut exiger que l'infraction soit commise en vilation fes mesures de securite, dans l'intention d obetenir des donnees informatiques ou dans une autre intention delictueuse, ou soit en relation avec un systeme informatique connecte a un autre systeme informatique.

Measures يرى أنها ضرورية من أجل اعتبارها جريمة جنائية ، وفقاً لقانونـــه الـــداخلي Its Domestic Law ، للولوج العمدي لكل أو لجزء من جهاز الكمبيوتر بدون حق. كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى ، أو أن ترتكب الجريمة في نظام كمبيوتر يكـــون متصلاً عن بعد بنظام كمبيوتر آخر".

وبرجوعنا للتقرير التفسيري [1] الخاص باتفاقية بودابست نلاحظ أن هذا التقرير يعتبر الولوج غير القانونى بمثابة الجريمة الرئيسية التي تنطوي على تهديد وتعد على أمن النظم أي السرية والسلامة والإتاحة للنظم والبيانات والمعلومات.

وعليه فان مجرد الدخول غير المصرح به ، بمعنى القرصنة أو الســطو أو الـــدخول غير المشروع في النظام المعلوماتية يعتبر فى حد ذاته غير قانوني [2] ، وذلك على أساس أن هذه الأفعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للنظم والبيانات ، كما أن هذا التدخل يمكن أن يترتب عليه الدخول الى بيانات سرية ، كذلك فإن هذا الـــدخول غيـــر المشروع يساعد القراصنة على ارتكاب جرائم معلوماتيـــة أخـــرى كـــالغش أو التزويـــر المعلوماتي.

1- Convention sur la cybercriminalite. STE.. no. 185, Rapport explicatif adopte 8 novembre2001, p17etS.

2- أمين أعزان ، الحماية الجنائية للتجارة الإلكترونية ، رسالة دكتوراه حقوق عين شمس ، 2005 ، ص85 وما بعدها.

المراجع

المراجع باللغة العربية:

- د . جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية ، سنة 2001.
- د . خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، 2009.
- د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994.
- د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دراسة مقارنة ، دار النهضة العربية،2001.
- د. نجيب حسني ، قانون العقوبات ، دار النهضة العربية ، 1987.

المراجع باللغة الفرنسية:

- Bibent (Michel), Le Droit du Traitement de l'Information, 2000.
- Davies (David), Computer Virus-The Major Computer Abuse Threat of 1988 ?, C.L.S.R. , 1988.
- Chamoux (Francoise), la loi sur la Fraude Informatique De Nouvelles Incriminations, Jcp,1988 , I, Doctrine 3321, No 9 ; Linant de bellefonds (xavier) & Hollande (Alain) Pratique du Droit de l'informatique, 1998.

Voir : Isabelle DE LAMBERTERIE, Preuve, conservation et archivage, in Une société sans papier ? Nouvelles technologies de l'information et droit de la preuve, La Documentation Française, Paris, 1990.

رسائل الدكتوراه:

- أمين أعزان ، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة ، رسالة دكتوراه حقوق عين شمس ، 2005.
- عمر محمد ابو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، رسالة دكتوراه حقوق عين شمس، 2005.
- شيماء عبد الغني محمد ، رسالة دكتوراه حقوق عين شمس ، الحماية الجنائية للتعاملات الإلكترونية ، 1992.

الأبحاث:

- د . علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة (بالتعاون مع مركز

الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة) في الفترة من 1-3 مايو 2000 ، المجلد الثاني ، ط3 ، 2004.

- د . محمد المرسي زهرة ، حجية التوقيع الإلكتروني في الإثبات ، بحث منشور بمجلة اتحاد المصارف العربية ، 1991 ، ص 114.